EXHIBIT 7

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;	Trend Micro Apex Central includes *a non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to: receive first vulnerability information* (e.g., a smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof, including associated information including, but not limited to information describing the actual vulnerabilities themselves, information describing endpoints that contain the particular operating system/application/version thereof, information describing policy/detection/remediation techniques for addressing the actual vulnerabilities relevant to the particular operating system/application/version thereof including signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) *from at least one first data storage* (e.g., memory on the at least one device storing a repository of the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof, etc.) *that is generated utilizing second vulnerability information* (e.g., a larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof, including associated information including, but not limited to information describing the possible vulnerabilities themselves, information describing the different operating systems/applications/versions thereof, information describing policy/detection/remediation techniques for addressing the potential vulnerabilities relevant to the different operating systems/applications/versions thereof including signature/policy updates for anti-virus/data loss prevention/intrusion-detection-system (IDS)/firewall software, where such vulnerabilities each include a security weakness, gap, or flaw that could be exploited by an attack or threat, etc.) *from at least one second data storage* (e.g., Common Vulnerabilities and Exposures (CVE) database, etc.) *that is used to identify a plurality of potential vulnerabilities* (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.)*;* **Note**: See, for example, the evidence below (emphasis added, if any):

EXHIBIT 7

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

"**About the Web Console**

The Apex Central web console provides centralized management, monitoring, and security visibility for all endpoints and users protected by Trend Micro products registered to the Apex Central server. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. The web console lets you administer the Apex Central network from any machine using a compatible web browser.

Apex Central supports the following web browsers:

- Microsoft Internet Explorer™ 11
- Microsoft Edge™
- Google Chrome™

Web Console Requirements

Resource	**Requirement**
Processor	300 MHz Intel™ Pentium™ processor or equivalent
RAM	128 MB minimum
Available disk space	30 MB minimum
Browser	Microsoft Internet Explorer™ 11, Microsoft Edge™, or Google Chrome™ Important: When using Internet Explorer to access the Apex Central web console, turn off Compatibility View.

Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 2-2 to 2-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"**Attack Discovery Detection Information**

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>Provides general information about threats detected by Attack Discovery

<table>
<tr><th>Data</th><th>Description</th></tr>
<tr><td>Generated</td><td>The date and time the managed product generated the data</td></tr>
<tr><td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr>
<tr><td>Endpoint</td><td>The name of the endpoint</td></tr>
<tr><td>Product</td><td>The name of the managed product or service</td></tr>
<tr><td>Managing Server Entity</td><td>The display name of the managed product server in Apex Central to which the endpoint reports</td></tr>
<tr><td>Product Version</td><td>The version of the managed product</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Risk Level</td><td>The risk level assigned by Attack Discovery</td></tr>
<tr><td>Pattern Version</td><td>The Attack Discovery pattern number for the detection type</td></tr>
<tr><td>Rule ID</td><td>The serial number of the detection rule</td></tr>
<tr><td>Rule Name</td><td>The rules which specify behaviors to be detected by Attack Discovery</td></tr>
<tr><td>Related Objects</td><td>The number of detections

Click the count to view additional details.

For more information, see Detailed Attack Discovery Detection Information on page B-11.</td></tr>
<tr><td>Generated (Local Time)</td><td>The time in the agent's local timezone when Attack Discovery detected the threat

The time is displayed with the UTC offset.</td></tr>
<tr><td>Instance ID</td><td>The detection ID assigned to the event</td></tr>
</table>
</td></tr>
</table>

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	<table><tr><td></td><td>Entries having the same instance ID belong under the same event.</td></tr><tr><td>Tactics</td><td>The MITRE ATT&CK™ tactic(s) detected For more information, see https://attack.mitre.org/tactics/enterprise/.</td></tr><tr><td>Techniques</td><td>The MITRE ATT&CK™ technique(s) detected For more information, see https://attack.mitre.org/techniques/enterprise/.</td></tr></table> *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page B-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "**Threat Encyclopedia** Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities. Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about: • Malware and malicious mobile code currently active or "in the wild" • Correlated threat information pages to form a complete web attack story • Internet threat advisories about targeted attacks and security threats • Web attack and online trend information • Weekly malware reports"

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 25-2 to 25-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) **Note**: As set forth below, managed product and child server information is equivalent to memory on the at least one device. "**Understanding the Apex Central Database** Apex Central uses the Microsoft SQL Server database (db_ApexCentral.mdf) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings. The Apex Central server establishes the database connection using a System DSN ODBC connection. The Apex Central installation generates this connection as well as the ID and password used to access db_ApexCentral.mdf. The default ID is sa. Apex Central encrypts the password. To maximize the SQL server security, configure any SQL account used to manage db_ApexCentral with the following minimum permissions: • dbcreator for the server role • db_owner role for db_ApexCentral Logs from managed products contribute to database expansion. Managed products send various log types to Apex Central." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 23-2 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
said first vulnerability information generated utilizing the second vulnerability information, by: identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and	Trend Micro Apex Central includes *said first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof) *generated utilizing the second vulnerability information* (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof)*, by: identifying at least one configuration* (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) *associated with a plurality of devices* (e.g., managed products and endpoints, etc.) *including a first device, a second device, and a third device* (e.g., a first, second, and third of the managed products and endpoints, etc.)*, and* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): "**Vulnerability attack** Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 3-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "Procedure 1. Go to **Administration > Security Agent Download**. 2. Select the operating system. • **Windows 64-bit**: Select to create a 64-bit MSI installation package for Apex One Security Agents • **Windows 32-bit**: Select to create a 32-bit MSI installation package for Apex One Security Agents • **Mac OS**: Select to create a ZIP installation package for Apex One (Mac) Security Agents"

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 9-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "**About Apex Central** Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Apex Central web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network. Apex Central enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy components, such as antivirus pattern files, scan engines, and antispam rules, throughout the network to ensure up-to-date protection. Apex Central allows both manual and pre-scheduled updates, and allows the configuration and administration of products as groups or as individuals for added flexibility." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 1-2 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the	Trend Micro Apex Central includes *determining that the plurality of devices* (e.g., managed products and endpoints, etc.) *is vulnerable to at least one accurately identified vulnerability* (e.g., one of a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *based on the identified at least one configuration* (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.)*, utilizing the second vulnerability information* (e.g., the larger "super-set" list of possible vulnerabilities relevant to different operating systems/applications/versions thereof) *that is used to identify the*

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td>plurality of potential vulnerabilities;</td><td>plurality of potential vulnerabilities (e.g., possible vulnerabilities relevant to different operating systems/applications/versions thereof, etc.);

<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

“The Threat Type column displays the following threat types.

<table>
<tr><th>Threat Type</th><th>Description</th></tr>
<tr><td>Ransomware</td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr>
<tr><td>Known Advanced Persistent Threat (APT)</td><td>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</td></tr>
<tr><td>Social engineering attack</td><td>Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr>
<tr><td>Vulnerability attack</td><td>Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr>
<tr><td>Lateral movement</td><td>Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr>
<tr><td>Unknown threats</td><td>Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer</td></tr>
</table>
</td></tr>
</table>

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>C&C callback</td><td>Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
<tr><td>identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more network monitors;</td><td>
Trend Micro Apex Central is configured to identify an occurrence (e.g., a positively-identified attack based on one of the known threat types, etc.) in connection with at least one of the plurality of devices (e.g., one of the managed products and endpoints, etc.), utilizing one or more network monitors (e.g., Trend Micro Apex Central, etc.);

<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

"The Threat Type column displays the following threat types.

<table>
<tr><th>Threat Type</th><th>Description</th></tr>
<tr><td><u>Ransomware</u></td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr>
<tr><td><u>Known Advanced Persistent Threat (APT)</u></td><td>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</td></tr>
<tr><td><u>Social engineering attack</u></td><td>Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr>
<tr><td><u>Vulnerability attack</u></td><td>Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr>
</table>
</td></tr>
</table>

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Lateral movement</td><td>Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr>
<tr><td>Unknown threats</td><td>Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer</td></tr>
<tr><td>C&C callback</td><td>Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"About Apex Central

Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Apex Central web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network. Apex Central enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy components, such as antivirus pattern files, scan engines, and antispam rules, throughout the network to ensure up-to-date protection. Apex Central allows both manual and pre-scheduled updates, and allows the configuration and administration of products as groups or as individuals for added flexibility."
</td></tr>
</table>

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 1-2 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
based on a packet analysis, determine that the at least one accurately identified vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and	Trend Micro Apex Central is configured to, *based on a packet analysis* (e.g., examining the actual content of network packets, etc.), de*termine that the at least one accurately identified vulnerability* (e.g., one of a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *of the at least one of the plurality of devices* (e.g., one of the managed products and endpoints, etc.) *is susceptible to being taken advantage of by the occurrence* (e.g., the positively-identified attack based on one of the known threat types, etc.) *identified in connection with the at least one of the plurality of devices* (e.g., one of the managed products and endpoints, etc.)*, utilizing the first vulnerability information* (e.g., the smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof)*; and* **Note**: See, for example, the evidence above (where applicable) and below (emphasis added, if any): "**Intrusion Prevention Rules** The **Intrusion Prevention Rules** screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>

To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns.
To sort the list of Intrusion Prevention Rules by column data, click a column heading.
To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule.”

Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

“Attack Discovery Detection Information

<u>Provides general information about threats detected by Attack Discovery</u>

<table>
<tr><th>Data</th><th>Description</th></tr>
<tr><td>Generated</td><td>The date and time the managed product generated the data</td></tr>
<tr><td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr>
<tr><td>Endpoint</td><td>The name of the endpoint</td></tr>
<tr><td>Product</td><td>The name of the managed product or service</td></tr>
<tr><td>Managing Server Entity</td><td>The display name of the managed product server in Apex Central to which the endpoint reports</td></tr>
<tr><td>Product Version</td><td>The version of the managed product</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Risk Level</td><td>The risk level assigned by Attack Discovery</td></tr>
<tr><td>Pattern Version</td><td>The Attack Discovery pattern number for the detection type</td></tr>
<tr><td>Rule ID</td><td>The serial number of the detection rule</td></tr>
<tr><td>Rule Name</td><td>The rules which specify behaviors to be detected by Attack Discovery</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Related Objects</td><td>The number of detections

Click the count to view additional details.

For more information, see Detailed Attack Discovery Detection Information on page B-11.</td></tr>
<tr><td>Generated (Local Time)</td><td>The time in the agent's local timezone when Attack Discovery detected the threat

The time is displayed with the UTC offset.</td></tr>
<tr><td>Instance ID</td><td>The detection ID assigned to the event

Entries having the same instance ID belong under the same event.</td></tr>
<tr><td>Tactics</td><td>The MITRE ATT&CK™ tactic(s) detected

For more information, see https://attack.mitre.org/tactics/enterprise/.</td></tr>
<tr><td>Techniques</td><td>The MITRE ATT&CK™ technique(s) detected

For more information, see https://attack.mitre.org/techniques/enterprise/.</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products</td></tr>
</table>

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities. Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about: • Malware and malicious mobile code currently active or "in the wild" • Correlated threat information pages to form a complete web attack story • Internet threat advisories about targeted attacks and security threats • Web attack and online trend information • Weekly malware reports" *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 25-2 to 25-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation	Trend Micro Apex Central is configured to *allow selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types* (e.g., firewall configuration, intrusion detection, etc.)*, including a firewall-based occurrence mitigation type* (e.g., firewall configuration including allowing network traffic to applications that Trend Micro has verified to be safe, etc.) and *an intrusion prevention system-based occurrence mitigation type* (e.g., intrusion detection including actions carried out on packets based on conditions set within an Intrusion Prevention Rule, etc.)*, across the plurality of devices* (e.g., managed products and endpoints, etc.) *for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities* (e.g., a subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.) *utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types* (e.g., firewall configuration, intrusion detection, etc.) *across the plurality of devices* (e.g., managed products and endpoints, etc.)*;*

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td>actions of the diverse occurrence mitigation types across the plurality of devices;</td><td>
<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

<table>
<tr><th>Consideration</th><th>Effect</th></tr>
<tr><td>Deployment planning</td><td><u>Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans</u>. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

“Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system.

…

Table 1. Product Status Information Data View

<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>
</td></tr>
</table>

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	<table><tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr></table> Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center "... 5. In the Certified Safe Software List section, configure the following: • **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. • **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. **Important**: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. 6. In the Exception section, manage the Exception Template List that applies to this policy only. ***The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List***. For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3). 7. Click **Save**."

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)

“Detailed Firewall Violation Information

Provides specific firewall configuration information on your network, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations”

<table>
<tr><th>Section</th><th>Settings</th></tr>
<tr><td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr>
<tr><td>Generated</td><td>The date and time the managed product generated the data</td></tr>
<tr><td>Product Entity/Endpoint</td><td>Depending on the related source:

• The display name of the managed product server in Apex Central
• The name or IP address of the endpoint Product</td></tr>
<tr><td>Product</td><td>The name of the managed product or service

Example: Apex One, ScanMail for Microsoft Exchange</td></tr>
<tr><td>Event Type</td><td>The type of event that triggered the detection

Example: intrusion, policy violation</td></tr>
<tr><td>Risk Level</td><td>The Trend Micro assessment of risk to your network

Example: High security, low security, medium security</td></tr>
<tr><td>Traffic/Connection</td><td>The direction of the transmission</td></tr>
</table>
</td></tr>
</table>

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Protocol</td><td>The protocol the intrusion uses

Example: HTTP, SMTP, FTP</td></tr>
<tr><td>Source IP</td><td>The source IP address of the detected threat</td></tr>
<tr><td>Endpoint Port</td><td>The port number of the endpoint under attack</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Target Application</td><td>The application the intrusion targeted</td></tr>
<tr><td>Description</td><td>The detailed description of the incident by Trend Micro</td></tr>
<tr><td>Action</td><td>The action taken by the managed product

Example: file cleaned, file quarantined, file passed</td></tr>
<tr><td>Detections</td><td>The total number of detections

Example: A managed product detects 10 violation instances of the same type on one computer

Detections = 10</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with recommended Intrusion Prevention rules based on your network performance and security priorities.</td></tr>
<tr><td>...</td><td>...</td></tr>
</table>
</td></tr>
</table>

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx

“Intrusion Prevention Rules

The Intrusion Prevention Rules screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

• To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns.
• To sort the list of Intrusion Prevention Rules by column data, click a column heading.
• To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule.”
Trend Micro Apex Central Administrator’s Guide, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

“The Threat Type column displays the following threat types.

<table>
<tr><th>Threat Type</th><th>Description</th></tr>
<tr><td>Ransomware</td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr>
<tr><td>Known Advanced Persistent Threat (APT)</td><td>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed</td></tr>
</table>
</td></tr>
</table>

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

<table>
<tr><th>Claim 1 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td><u>and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</u></td></tr>
<tr><td>Social engineering attack</td><td>Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr>
<tr><td>Vulnerability attack</td><td>Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr>
<tr><td>Lateral movement</td><td>Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr>
<tr><td>Unknown threats</td><td>Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer</td></tr>
<tr><td>C&C callback</td><td>Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
<tr><td>wherein the at least one configuration involves at least one operating system.</td><td>Trend Micro Apex Central is configured wherein the at least one configuration (e.g., Microsoft Windows 64-bit, Windows 32-bit, and Mac OS, or an application/version thereof, etc.) involves at least one operating system.

<u>Note</u>: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

"Vulnerability attack</td></tr>
</table>

PRELIMINARY CLAIM CHART

Patent No. 10,609,063, Claim 1: Trend Micro Apex Central

Claim 1 Elements	Applicability
	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems (pg 3-10)" *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 3-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "Procedure 1. Go to **Administration > Security Agent Download**. 2. Select the operating system. • **Windows 64-bit**: Select to create a 64-bit MSI installation package for Apex One Security Agents • **Windows 32-bit**: Select to create a 32-bit MSI installation package for Apex One Security Agents • **Mac OS**: Select to create a ZIP installation package for Apex One (Mac) Security Agents" *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 9-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

Caveat: The notes and/or cited excerpts utilized herein are set forth for illustrative purposes only and are not meant to be limiting in any manner. For example, the notes and/or cited excerpts, may or may not be supplemented or substituted with different excerpt(s) of the relevant reference(s), as appropriate. Further, to the extent any error(s) and/or omission(s) exist herein, all rights are reserved to correct the same in connection with any subsequent correlations.